Quantum Information and Computation, Vol. 0, No. 0 (2003) 000–000

ON THE SECURITY OF $\alpha\eta$: RESPONSE TO 'SOME ATTACKS ON QUANTUM-BASED CRYPTOGRAPHIC PROTOCOLS'

Horace P. Yuen,[a] Ranjith Nair, Eric Corndorf, Gregory S. Kanter, and Prem Kumar
Center for Photonic Communication & Computing,
Department of Electrical Engineering & Computer Science, Department of Physics & Astronomy,
Northwestern University, Evanston, IL, 60208, USA.

Received (received date)
Revised (revised date)

Lo and Ko in [1] have developed some attacks on the cryptosystem called $\alpha\eta$ [2], claiming that these attacks undermine the security of $\alpha\eta$ for both direct encryption and key generation. In this paper, we show that their arguments fail in many different ways. In particular, the first attack in [1] requires channel loss or length of known-plaintext that is exponential in the key length and is unrealistic even for moderate key lengths. The second attack is a Grover search attack based on 'asymptotic orthogonality' and was not analyzed quantitatively in [1]. We explain why it is not logically possible to "pull back" an argument valid only at $n = \infty$ into a limit statement, let alone one valid for a finite number of transmissions n. We illustrate this by a 'proof' using a similar asymptotic orthogonality argument that coherent-state BB84 is insecure for *any* value of loss. Even if a limit statement is true, this attack is *a priori* irrelevant as it requires an indefinitely large amount of known-plaintext, resources and processing. We also explain why the attacks in [1] on $\alpha\eta$ as a key-generation system are based on misinterpretations of [2]. Some misunderstandings in [1] regarding certain issues in cryptography and optical communications are also pointed out. Short of providing a security proof for $\alpha\eta$, we provide a description of relevant results in standard cryptography and in the design of $\alpha\eta$ to put the above issues in the proper framework and to elucidate some security features of this new approach to quantum cryptography.

Communicated by: to be filled by the Editorial

1 Introduction

In [1], Lo and Ko describe, without quantitative calculations, some attacks on the direct encryption protocol of [2], interpreted by them also as a key generation scheme. They draw the firm conclusion that our protocol is fundamentally insecure, that these attacks were neglected by us as they are "outside the original design," and that they "can, to some extent, be implemented with current technology." We contend that the strength and weakness of our scheme have been totally misrepresented in [1], which does not analyze the relevant cryptographic problems in a meaningful framework. Although we have already commented briefly on the attacks of [1] in [3] and [5], and some related comments are given by Hirota et al in [6], [1] is still often quoted without also referring to our partial rejoinder. Thus, we feel it appropriate that a specific response to [1] be made in a complete paper. In particular, we would like to

[a]yuen@eecs.northwestern.edu

clear up at the same time many issues in the practical use of quantum cryptography and in the properties of $\alpha\eta$ that have so far not been elucidated in the literature. We do not attempt to give a complete security proof of $\alpha\eta$ in this paper. Such a proof is not available and is the subject of ongoing research. See [4] for recent results. Nevertheless, it is possible to refute the arguments of Lo and Ko taken by themselves, and this will be the main aim of this paper.

First of all, we note that the attacks in [1] do not contradict our claim in [2] that $\alpha\eta$ encryption provides *exponential complexity-based* security against known-plaintext attacks using a particular 'assisted' brute-force search. See [2] or alternatively, [4] for a more detailed description. Although we mention the possibility of key generation with $\alpha\eta$, we do not present an explicit scheme to do so in [2]. The authors of [1] assume that the protocol of [2] works without any additions or modifications for key generation, which was not claimed by us at all. While they arrive at attacks that purport to show that $\alpha\eta$ is insecure in the information-theoretic sense against known-plaintext attacks — already believed by us to be quite possible [3] — we claim that the two attacks in [1] do not conclusively prove insecurity of any finite-n system. Proof is important in this quantum situation because $\alpha\eta$ falls outside the class of classical nonrandom ciphers for which known-plaintext attacks can be proved to succeed. But perhaps more significantly, the Lo-Ko attacks are unrealistic in the *fundamental* sense of having exponential complexity and requiring an exponential amount of resources. In Section 2.2, we bring out the *important point* that, in contrast to other kinds of complexity, exponential complexity offers realistic security as good as unconditional security.

We shall explain fully our criticisms of [1] in the course of this paper. In this introductory section, we will lay out three major general defects in [1] which in our opinion are also implicit in various papers on theoretical quantum cryptography. We will later have occasion to indicate specific points where these defects arise when we reply in detail in Section 4 to the attacks in [1].

In the *first* place, vague qualitative arguments are often offered as rigorous proofs, while at the same time not giving precise conditions under which a result is claimed to be valid. In [1], there are even several claims made without any argument at all. Rigorous proofs are important in quantum cryptography because the main superiority it claims over standard cryptography is the possibility of rigorous proof of security, unconditional or otherwise. A more subtle point is that many arguments, including one in [1], rely on statements valid *at* $n = \infty$ which *cannot* be cast into *limiting* statements on the relevant quantities. Indeed, limit and continuity questions at $n = \infty$ are especially subtle in quantum mechanics owing to the nonseparable Hilbert space, i.e., a Hilbert space with an uncountable basis, that arises when $n = \infty$. One pitfall of such a leap of faith is illustrated in Section 5.

Secondly, strong claims are made with no actual numbers or numerical ranges indicated for the validity of the results. Thus, results are often claimed to be valid asymptotically as the number of bits n in a sequence goes to infinity, without any estimate on the convergence rate. Such limiting results alone are of no use to an experimentalist or designer of a *real* system. As security proofs, they offer no quantitative guarantee of any kind on an actual realistic system where n is often not even very large. As attacks, they imply nothing about the level of insecurity of any finite n system without convergence-rate estimates. Thus, showing a scheme to be insecure simply as a limiting statement when $n \to \infty$ has no practical implication. (See Section 4 for a complete discussion.) A related point is with regard to the realistic

significance of quantities that vary exponentially with respect to some system parameter. Thus, consideration of attacks, as is the case in one attack in [1], that succeed only when the channel-transmittance (the output-to-input power ratio) $\eta \sim 2^{-|K|}$, where $|K|$ is the key length, is seen to be practically irrelevant by plugging in typical numbers for $|K|$. More significantly, attacks that require exponential resources or processing like those in [1] are irrelevant in a fundamental sense, because the situation *cannot* be changed by technological advances, similar to the case of unconditional security.

These points are important because security in cryptography is a quantitative issue. For example, in quantum key generation, the exact amount of Eve's uncertainty determines how much key is generated. To ensure that one generates a sufficiently large key, it is not sufficient to use qualitative arguments that are valid only at extreme limits, since they may break down quantitatively in realistic systems.

Thirdly, the general approach to quantum cryptography underlying $\alpha\eta$, called 'Keyed Communication in Quantum Noise' (KCQ) [3], is not well understood. In particular, the various and distinct issues in connection with direct encryption and key generation with (or even without) a secret key, which have to be clearly delineated for a proper analysis, are lumped together in [1], generating considerable confusion even in the context of classical cryptography. Since our approach is novel, this current situation is perhaps understandable. While the full story of this field of research is still to be understood, some clarifications can be made to clear up the various confusions.

In addition to the above, some specific details of implementation of $\alpha\eta$ are also misconstrued in [1]. Along with responding to the Lo-Ko arguments, one main purpose of this paper is to provide the proper framework for security analysis of $\alpha\eta$, for direct encryption as well as key generation. It is *not* the purpose of this paper to provide any detailed security analysis of $\alpha\eta$, which is a huge undertaking and an on-going effort. However, we will indicate the many features that make $\alpha\eta$ uniquely interesting and useful at various places in the paper.

The plan of this paper is as follows: In Section 2, we provide an outline of relevant results and facts in symmetric-key cryptography, which are not well-known. Our statements on direct encryption cryptography in this paper refer only to the symmetric-key case, and not to public-key cryptography. In fact, public-key cryptography is not used for encryption of data sequences of more than a few hundred bits owing to its slow speed. We discuss in a subsection the current knowledge regarding security against known-plaintext attacks in standard cryptography and discuss the concepts of a *random cipher* and a *nondegenerate* cipher. Much of this subsection as well as Appendix A are our own contributions. They contain subtle distinctions needed to precisely state important results, and may be regarded as providing the basic framework in which to view known-plaintext attacks on $\alpha\eta$ or any other randomized encryption system. In Section 3, we review our $\alpha\eta$ scheme and the different security issues associated with its use in direct encryption and key generation. In Section 4, the Lo-Ko attacks and their specific criticisms are explained and responded to, both specifically and generally in view of the above-mentioned defects. It will be shown that their arguments are deficient in many different ways. To illustrate the fallacy of the 'asymptotic orthogonality' argument, a 'proof' that coherent-state BB84 using a classical error-correction code is insecure for any loss, no matter how small, is presented in Section 5. Various other misconceptions in [1] are listed in Section 6. A brief summary of our conclusions is given in Section 7.

2 Cryptography

2.1 Direct Encryption

We assume that the basics of symmetric-key data encryption are known to the reader (See, e.g., [7, 8]). Thus, the n-symbol long plaintext is denoted by the random variable X_n, the corresponding ciphertext is denoted Y_n and the secret key is denoted K. In standard cryptography, one usually deals with *nonrandom ciphers*, namely those cryptosystems for which the conditional entropy

$$H(Y_n|KX_n) = 0. \tag{1}$$

Thus, the plaintext and key uniquely determine the ciphertext. In such a case, X_n and Y_n are usually taken to be from the same alphabet. Note that in this paper, equations involving n as a parameter are assumed to be valid for all n unless stated otherwise. Ciphers for which Eq.(1) is relaxed so that the same plaintext may be mapped for a given key to many different ciphertexts, perhaps drawn from a different alphabet than X_n, will be called random ciphers. Thus, a *random cipher* is defined by

$$H(Y_n|KX_n) \neq 0. \tag{2}$$

Such ciphers are called 'privately randomized ciphers' in Ref. [8] as the different ciphertexts Y_n for a given X_n are obtained by privately (i.e., in an unkeyed fashion known only to the sender Alice) randomizing on a specific Y_n. We will just call such a cipher a random cipher (Note that 'random cipher' is used in a completely different sense by Shannon [9]). For both random and nonrandom ciphers, we enforce the condition that the plaintext be recoverable from the ciphertext and the key, i.e.,

$$H(X_n|KY_n) = 0. \tag{3}$$

A detailed quantitative characterization of classical and quantum random ciphers is available in [4].

By *standard cryptography*, we shall mean that Eve and Bob both observe the same ciphertext random variable, i.e., $Y_n^{\mathrm{E}} = Y_n^{\mathrm{B}} = Y_n$. Note that in such a standard cipher, random or nonrandom, the following *Shannon limit* [8, 9] applies:

$$H(X_n|Y_n) \leq H(K). \tag{4}$$

By *information-theoretic security* on the data, we mean that Eve cannot pin down uniquely the plaintext from the ciphertext, i.e.,

$$H(X_n|Y_n) \neq 0. \tag{5}$$

The *level* of such security is quantified by $H(X_n|Y_n)$. Shannon has defined *perfect security* [9] to mean that the plaintext is statistically independent of the ciphertext, i.e.,

$$H(X_n|Y_n) = H(X_n). \tag{6}$$

We shall use *near-perfect* security to mean $H(X_n|Y_n) \sim H(X_n)$. Security statements on ciphers are naturally made with respect to particular possible attacks. We will discuss the usual cases of ciphertext-only attack, known-plaintext attack, and statistical attack in the next subsection. We now turn to key generation.

2.2 Key Generation

The objective of key generation is to generate fresh keys. By a *fresh* key, we mean a random variable K^g shared by the users from processing on X_n for which

$$H(K^g|KY_n^E) \sim H(K^g) \tag{7}$$

for *some* n. Here K is any secret key used in the key generation protocol. In other words, one needs to generate *additional* randomness statistically independent of previous shared randomness such as a secret key used in the protocol. The two major approaches to key generation are via classical noise [10] and BB84-type [11] quantum cryptography. With the advent of quantum cryptography, the term 'unconditional security' has come to be used, unfortunately, in many possible senses. By *unconditional security*, we shall mean near-perfect information-theoretic security against all attacks consistent with the known laws of quantum physics.

Using Eq. (3), it is easily seen that, in standard cryptography, X_n, or any publicly announced function thereof, cannot serve as fresh key. This is because all the uncertainty in X_n is derived from K, however long n is, and therefore $H(K^g|KY_n) = 0$.

While key generation is impossible in standard cryptography, it becomes possible in principle in a situation where $Y_n^E \neq Y_n^B$. This necessary condition must be supplemented by a condition for *advantage creation* [3], e.g.,

$$H(X_n|KY_n^E) > H(X_n|KY_n^B). \tag{8}$$

In (8), the key K is conceptually granted to Eve after her measurements to bound the information she may possibly obtain by any collective classical processing that takes advantage of the correlations introduced by K. We mention here that even when there is no *a priori* advantage, provided $Y_n^B \neq Y_n^E$, advantage may often be created by *advantage distillation*, as e.g., through post-detection selection so that Eq.(8) is satisfied for the selected results. Keyed Communication in Quantum Noise, called KCQ in [3] and hereafter, provides one way of creating advantage for fresh key generation from the performance difference between the optimal quantum receivers designed with and without knowledge of the secret key. Some of the advantages of such an approach to key generation would be indicated later, and further details can be found in [3, 12].

Even when information-theoretic security does not obtain, so that the data or the key is in fact uniquely determined by the ciphertext (we shall see in Subsection 2.4 that this is the usual situation in standard cryptography when the plaintext has known nonuniform statistics), we may still speak of *complexity-based* security. This refers to the amount of computation or resources required to find the unique plaintext X_n or key K corresponding to the observed Y_n. In practice, forcing a large amount of computation on Eve can provide very effective security. In fact, standard ciphers owe their widespread use to the absence of known efficient algorithms that can find the unique key or plaintext from the ciphertext, with or without some known plaintext. Note that the security of a system is especially good if the complexity goes exponentially in $|K|$, resulting in a search problem that *cannot* be efficiently handled even by a quantum computer. In contrast to merely 'hard' problems such as factoring integers or even NP-complete problems, for which complexity is not quantified, *exponential complexity* is a guarantee of realistic security *as good as unconditional security*. This is because a quantity

that is exponential in a system parameter can easily become so large as to be impossible to achieve. For example, it is a fact as certain as any physical law that one cannot have 10^{600} beamsplitters (See our response to the first attack of Lo and Ko in Section 4.) on the earth, or in the whole known universe for that matter — this can be seen merely from size considerations. Similar remarks hold for exponential computing time requirements. However, neither $\alpha\eta$ nor any standard cipher has been proven to require exponential resources to break.

2.3 Classes of attacks in quantum cryptography

In our KCQ approach, we conceptually grant a copy of the transmitted state to Eve for the purpose of bounding her information. Thus, there is no need of considering what kind of probe she uses. For further details, see [3, 12]. Accordingly, we will classify attacks a little differently from the usual case in BB84 protocols, basing our classification only on the quantum measurement or processing Eve may make.

By an *individual attack*, we mean one where the same measurement is made in every qubit/qumode and the results are processed independently of one another. Obviously, the latter is an artificial and unrealistic constraint on an attack, but analyses under this assumption are standard for BB84. In this connection, we note that in the BB84 literature, one often finds individual attacks being defined only by Eve's qubit-by-qubit probes and measurements, but with the actual analysis of such attacks being carried out with the *further assumption* that no classical collective processing is used, so that Eve has independent, identically distributed (iid) random variables on her bit estimates. This assumption renders the results rather meaningless, as Eve can easily jointly process the quantum measurement results to take advantage of the considerable *side information* available to her from announcements on the classical public channel. It is a subtle task to properly include such side information in the security proofs of BB84-type protocols, one that we will elaborate upon in future papers. However, it is this definition of individual attack that has been used for our information-theoretic security claims in [2].

By a *collective attack*, we mean one where the same measurement is made in every qubit/qumode but where joint classical processing of the results is allowed. Conceptually, one may also consider the most general attacks on classical systems to be in this class. We will refer to a particular collective attack on $\alpha\eta$ using heterodyne or phase measurement on each qumode later in this paper. Note also that encryption of a known plaintext with all possible keys followed by comparison of the result to the observed mode-by-mode measurement result Y_n^E (i.e. a *brute-force search*) is a collective attack, since the correlations between the ciphertext symbols introduced during encryption are being used. Note that our use of the term "collective attack" is different from the BB84 case, due to the fact that there is no need to account for probe setting in our KCQ approach. Finally, for us, a *joint attack* refers to one where a joint quantum measurement on the entire sequence of qubits/qumodes is allowed. This is the most general attack in the present circumstance, and must be allowed in any claim of unconditional security.

2.4 Security against known-plaintext attacks and statistical attacks

In this subsection, we describe some results in classical cryptography that are not readily available in the literature. For a standard cipher, the conditional entropy $H(X_n|Y_n)$ describes the level of information-theoretic security of the data X_n, and $H(K|Y_n)$ describes

the information-theoretic security of the key. The attacks considered in cryptography are ciphertext-only attacks, and known-plaintext or chosen-plaintext attacks. There is in the literature an ambiguity in the term 'ciphertext-only attack' regarding whether the *a priori* probability distribution $p(X_n)$ of the data is considered known to the attacker or is completely random to her. To avoid confusion, we will use the term *ciphertext-only attack* to refer to the case where $p(X_n)$ is completely random to Eve, *statistical attack* to refer to the case when some information on X_n in the form of a nonuniform $p(X_n)$ is available to Eve, *known-plaintext attack* to refer to the case when some specific X_n is known to Eve, and *chosen-plaintext attack* to refer to the case when some specific X_n is chosen by Eve. Generally, our results referring to known-plaintext attacks are valid in their qualitative conclusions also for chosen-plaintext attacks. (Note that we are restricting ourselves to private-key cryptography – This is not generally true in public-key cryptography.) Therefore, our use of the term 'known-plaintext attack' may be taken to include chosen-plaintext attacks also, for symmetric-key direct encryption.

In standard cryptography, one typically does not worry about ciphertext-only attack on nonrandom ciphers, for which Eq. (4) is satisfied with equality for large n for the designed key length $|K| = H(K)$ under some 'nondegeneracy' condition [13]. In such situations, it is also the case that $H(K|Y_n) = H(K)$ so that no attack on the key is possible [13]. However, under statistical and known-plaintext attacks, this is no longer the case and Eve can launch an attack on the key and use her resulting information on the key to get at future data. Indeed, it is such attacks that are the focus of concern in standard ciphers such as the Advanced Encryption Standard (AES). For statistical attacks, Shannon [9] characterized the security by the *unicity distance* n_0 *(for statistical attacks)*, which is defined to be the input data length at which $H(K|Y_{n_0}) = 0$. For a nonrandom cipher defined by (1), he derived an estimate on n_0 that is *independent* of the cipher in terms of the data entropy. This estimate is, unfortunately, not a rigorous bound. Indeed, one of the inequalities in the chain goes in the wrong direction in the derivation, although it works well empirically for English where $n_0 \sim 25$ characters. Generally, it is easy to see that a finite unicity distance exists only if, for some n, there is no *redundant key use* in the cryptosystem, i.e., no plaintext sequence X_n is mapped to the same ciphertext Y_n by more than one possible key value. With redundant key use, one cannot pin down the key but it seems one also could not enhance the system security either, and so is merely wasteful. The exact possibilities will be analyzed elsewhere. A nonrandom cipher is called *nondegenerate* in this paper if it has no redundant key use either at some finite n or for $n \to \infty$. A *random* cipher will be called nondegenerate when each of its nonrandom reductions is nondegenerate (See [4]). Under the condition

$$\lim_{n\to\infty} H(Y_n|X_n) = H(K), \tag{9}$$

which is similar but not identical to the definition of a 'nondegenerate' cipher given in [13], one may show that, when (1) holds, one has

$$\lim_{n\to\infty} H(K|X_nY_n) = 0. \tag{10}$$

In general, for a nonrandom cipher, we define a *nondegeneracy distance* n_d to be the smallest n such that

$$H(Y_n|X_n) = H(K) \tag{11}$$

holds, with $n_d = \infty$ if (9) holds and there is no finite n satisfying (11). Thus, a nonrandom cipher is nondegenerate in our sense if it has a nondegeneracy distance, finite or infinite. In general, of course, the cipher may be *degenerate*, i.e., it has no nondegeneracy distance. We have the result given by Proposition A of Appendix A that, *under known-plaintext attack, a nonrandom nondegenerate cipher is broken at data length* $n = n_d$. This is also the minimum length of data needed to break the cipher for any possible known-plaintext X_n. Many ciphers including the one-time pad and LFSRs (linear feedback shift registers [7]) have finite n_d. For chosen-plaintext attacks, the above definitions and results apply when the random variable X_n is replaced by a specific $X_n = x_n$.

The above result has not been given in the literature, perhaps because $H(K|X_nY_n)$ has not been used previously to characterize known-plaintext attacks. But it is assumed to be true in cryptography practice that K would be pinned down for sufficiently long n in a nonrandom 'nondegenerate' cipher. However, there is *no* analogous result on random ciphers, since under randomization Eq. (1), and usually (11) also, does not hold for any n.

The following result is similar to one in [13, 14]. The homophonic substitution algorithms provided in these references work also for finite sequences, and may result in data compression rather than data expansion depending on the plaintext.

Proposition B

In a statistical attack on nonuniform iid X_n, homophonic substitution randomization [13, 14] on a nonrandom nondegenerate cipher can be used to convert the attack into a ciphertext-only one, thus completely protecting the key.

This reduction does not work for known-plaintext attacks. The problem of attacking a symmetric-key random cipher has received limited attention because they are not used in practice due to the associated reduction in effective bandwidth or data rate, and also due to the uncertainty on the actual input statistics needed for homophonic substitution randomization. Thus, the quantitative security of random ciphers against known-plaintext attacks is not known theoretically or empirically, although in principle random ciphers could defeat statistical attacks according to Proposition B. All that is clear is that random ciphers are harder to break than the corresponding nonrandom ones, because a given pair (X_n, Y_n) may arise from more possible keys due to the randomization. See ref. [4] for a detailed elucidation.

If a random cipher is nondegenerate, we say it has *information-theoretic security against known-plaintext attacks* when

$$\inf_n H(K|X_nY_n) > 0, \tag{12}$$

i.e., if $H(K|X_nY_n)$ cannot be made arbitrarily small whatever n is. The actual level of the information-theoretic security is quantified by the left side of (12). As in the nonrandom case, only for a nondegenerate cipher, i.e., one with no redundant key use, is it *meaningful* to measure key security with entropy. It is *possible* that some random ciphers possess such information-theoretic security. See Appendix A.

We define the *unicity distance* n_1 *for known-plaintext attacks*, for both nondegenerate

random and nonrandom ciphers, as the smallest n, if it exists, for which

$$H(K|X_nY_n) = 0. \tag{13}$$

The unicity distance n_1 is defined to be infinity if (13) holds for $n \to \infty$. Any cipher with information-theoretic security against known-plaintext attacks has no unicity distance n_1. For a nondegenerate nonrandom cipher, we have shown in Appendix A that $n_1 = n_d$. We shall see in the next section that $\alpha\eta$ can be considered a random cipher in the above sense under collective attacks, but with no reduction in effective data rate. (Recall that collective attacks are the most general in classical ciphers.) Thus, the statement in [1] that "known-plaintext attacks are rather standard and were successfully launched against both the Germans and the Japanese in World War II" is an oversimplification, since the ciphers referred to in it were nonrandom.

3 $\alpha\eta$ Direct Encryption and Key Generation

Consider the original experimental scheme $\alpha\eta$ (called Y-00 in Japan) as described in [2] and depicted in Fig. 1. Alice encodes each data bit into a coherent state in a *qumode*, i.e., an infinite-dimensional Hilbert space (the terminology is analogous to the use of *qubit* for a two-dimensional Hilbert space), of the form (we use a single qumode representation rather than a two-qumode one for illustration)

$$|\alpha_\ell\rangle = |\alpha_0(\cos\theta_\ell + i\sin\theta_\ell)\rangle \tag{14}$$

where α_0 is real, $\theta_\ell = 2\pi\ell/M$, and $\ell \in \{0, ..., M-1\}$. The M states are divided into $M/2$ basis pairs of antipodal signals $\{|\pm\alpha_\ell\rangle\}$ with $-\alpha_\ell = \alpha_{\ell+M/2}$. A seed key K of bit length $|K|$ is used to drive a conventional encryption mechanism whose output is a much longer running key K' that is used to determine, for each qumode carrying the bit $b\{= 0, 1\}$, which pair $\{|\pm\alpha_\ell\rangle\}$ is to be used. The bit b could either be part of the plaintext in a direct encryption system (as is the case in [2]) or it could be a raw key bit from a random number generator. Bob utilizes a quantum receiver to decide on b knowing which particular pair $\{|\pm\alpha_\ell\rangle\}$ is to be discriminated. On the other hand, Eve needs to pick a quantum measurement for her attack in the absence of the basis knowledge provided by the seed or running key. The difference in their resulting receiver performances is a quantum effect that constitutes the ground, as we shall see in subsequent subsections, both for making $\alpha\eta$ a random cipher for direct encryption, and for possible advantage creation vis-a-vis key generation. To avoid confusion, we shall use the term '$\alpha\eta$' to refer only to the direct encryption system following our practice in [2]. When we want to use the same system as part of a key generation protocol, we shall refer to it as '$\alpha\eta$-Key Generation' or '$\alpha\eta$-KG'. We discuss $\alpha\eta$ and $\alpha\eta$-KG in turn in the next two subsections.

Note that since the quantum-measurement noise is irreducible, such advantage creation may result in an unconditionally secure key-generation protocol. In contrast, in a classical situation including noise, the simultaneous measurement of the amplitude and phase of the signal, as realized by heterodyning, provides the general optimal measurement for both Bob and Eve; thus preventing any advantage creation under our approach that grants Eve a copy of the state for the purpose of bounding her information. We may remark that since a

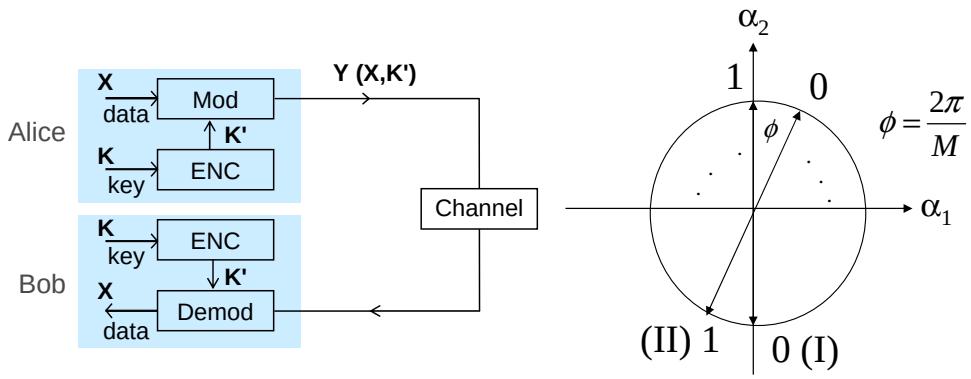

Fig. 1. Left:Overall schematic of the $\alpha\eta$ scheme. Right: Depiction of $M/2$ bases with interleaved logical state mappings.

discrete quantum measurement is employed by the users, $\alpha\eta$ and $\alpha\eta$-KG are *not* continuous-variable quantum cryptosystems. In particular, their security is not directly derived from any uncertainty relation for observables with either continuous or discrete spectrum.

3.1 $\alpha\eta$ Direct Encryption

Let $X_n, Y_n^{\rm E}, Y_n^{\rm B}$ be the classical random vectors describing respectively the data, Eve's observation, and Bob's observation. Eve may make any quantum measurement on her copy of the quantum signal to obtain $Y_n^{\rm E}$ in her attack. One then considers the error in her estimation of X_n. As an example, consider the attack where Eve makes a heterodyne measurement or a phase measurement on each qumode [3, 5]. Under such an attack, $\alpha\eta$ becomes essentially a classical random cipher (in the sense of Section 2), because it satisfies

$$H(X_n|Y_n^E, K) \sim 0 \tag{15}$$

along with Eq. (2) for the experimental parameters of [2, 15, 16, 17]. Under Eq. (15), Eq. (4) also obtains and the data security is no better than $|K|$ as in all standard symmetric key ciphers. Still, heterodyning by Eve does not reduce $\alpha\eta$ to a classical nonrandom stream cipher, as claimed in [18]. Rather, it becomes a *random cipher* as already pointed out in [3]. For each transmitted qumode, the plaintext alphabet is $\{0, 1\}$ and the ciphertext alphabet is any point on the circle of Fig. 1 when a phase measurement is made by Eve, and is any point in the plane when a heterodyne measurement is made. Note that the ciphertext *alphabet* depends on what quantum measurement is made by the attacker. However, it can at most be reduced to an M-ary one by collapsing the continuous outcomes into M disjoint sets. This is so because such an alphabet is the smallest possible ciphertext alphabet such that it is possible to decrypt for *every* possible value of ciphertext and key. We have elaborated on this point in Section 5 of [4]. Hence, $\alpha\eta$ is a random cipher against attacks on the key, and cannot be reduced to an additive stream cipher, which is nonrandom. When it is forced to become nonrandom, even just for Bob, it becomes noisy. See our reply [5] to the attack in [18] for more details. Also see their subsequent response [19] based on a confusion regarding the interpretation of Eq.(15), which is valid for our $\alpha\eta$ system of [2]. Further elaboration is available in [4].

Observe that the randomization in $\alpha\eta$ can be accomplished classically in principle, but not in current practice. This is because true random numbers can only be generated physically, not by an algorithm, and the practical rate for such generation is many orders of magnitude below the $\sim$ Gbps rate in our experiments where the coherent-state quantum noise does the randomization *automatically*. Furthermore, our physical "analog" scheme does not sacrifice bandwidth or data rate compared to other known randomization techniques. This is because Bob resolves only two, not M possibilities. Another important point with regard to physical cryptosystems like $\alpha\eta$, whether random or nonrandom, is that they require the attacker to make *analog* or at least M-ary observations, i.e., to attack the system at the *physical* level, even though the data transmitted is binary. In particular, as indicated above, it is impossible to launch a known-plaintext attack on the key using just the binary output, available for instance at a computer terminal.

While the original $\alpha\eta$ scheme of Fig. 1 is a random cipher under collective attacks made without knowledge of the key K, or more generally, under qumode-by-qumode measurements that can vary from qumode to qumode, it is still a nonrandom cipher in the sense of quantum states. See also ref. [4]. The technique called Deliberate Signal Randomization (DSR) described in [3] would make it a random cipher even with respect to quantum states. This amounts to randomizing (privately in the sense of [8]) the state transmitted so as to cover a half-circle around the basis chosen by the running key. The security of such ciphers is an open area of research. While we will not delve into the details of DSR in this paper, it may be mentioned that at the mesoscopic signal levels used in [2, 15, 16, 17], DSR with an error-correcting code on top may be expected to induce many errors for Eve while Bob remains essentially error-free. The reason is similar to that for Eq. (4) in Ref. [5], with advantage for Bob due to the optimal receiver performance difference described in the next subsection and in [3]. Thus, information-theoretic security is expected [3] for the key, and at a level far exceeding the Shannon limit for the data, when DSR is employed on $\alpha\eta$. Instead of DSR, a keyed 'mapper' that varies the mapping from the running key to the basis from qumode to qumode can also be employed, including perhaps a polarity (0 or 1) bit to enhance security. Even with the original $\alpha\eta$, it can be expected that the randomization or coherent-state noise would increase the unicity distance n_1 compared to the ENC box alone used as a cipher. Further details can be found in [4].

For the direct-encryption experiments in Refs. [2, 15, 16, 17], we have claimed "unconditional" security only against ciphertext-only individual attacks. We have claimed only *exponential complexity-based* security against assisted brute-force search (See [4]) known-plaintext attacks, which is more than the security provided just by the ENC box of Fig.1 [5]. However, information-theoretic security, even at the near-perfect level for both the key and the data, is possible with additional techniques or CPPM-type schemes described in [3]. Detailed treatment will be given in the future. But see also ref. [4].

We summarize the main known advantages of $\alpha\eta$ compared to previous ciphers:

(1) It has more assisted brute-force search complexity for attacks on the key compared to the case when the quantum noise is turned off. For an explicit claim, see [4].

(2) It may, especially when supplemented with further techniques, have information-theoretic security against known-plaintext attacks that is not possible with nonrandom ciphers.

(3) With added Deliberate Signal Randomization (DSR), it is expected to have information-theoretic security on the data far exceeding the Shannon limit.

(4) It has high-speed private true randomization (from quantum noise that even Alice does not know), which is not possible otherwise with current or foreseeable technology.

(5) It suffers no reduction in data rate compared to other known random ciphers.

(6) The key cannot be successfully attacked from a computer terminal with bit outputs, as is possible with standard ciphers.

3.2 $\alpha\eta$ Key Generation

One needs to clearly distinguish the use of such a scheme for key generation versus data encryption. It may first appear that if the system is secure for data encryption, it would also be secure for key generation if the transmitted data are subsequently used as new key. It seems to be the view taken in [1, 18, 20] that we have made such a claim, which we have not. The situation may be delineated as follows. Following the notations of the last subsection, Eve may make any quantum measurement on her copy of the quantum signal to obtain $Y_n^{\rm E}$ in her attack. Such a measurement is made *without the knowledge of* K. It is then used together with the value of K to estimate the data X_n. Although Eve is not actually given K after her measurements, we give it to her *conceptually* for the purpose of bounding her information. The conditions for unconditional security are complicated, and to satisfy them one needs to extend $\alpha\eta$-KG in different possible ways, such as DSR and CPPM described in [3]. However, against attacks with a fixed qumode measurement, Eq. (8) is sufficient and can be readily seen to hold as follows.

With $S \equiv |\alpha_0|^2$ being the average photon number in the states (11), the bit-error rate for Bob with the optimum quantum receiver [22] is

$$P_b = \frac{1}{4} e^{-4S}. \tag{16}$$

The bit-error rate for heterodyning, considered as a possible attack, is the well-known Gaussian result

$$P_b^{\rm het} \sim \frac{1}{2} e^{-S}, \tag{17}$$

and that for the optimum-phase measurement tailored to the states in (14) is

$$P_b^{\rm ph} \sim \frac{1}{2} e^{-2S} \tag{18}$$

over a wide range of S. The difference between Eq. (16) and Eq. (17-18) allows key generation at any value of S if n is long enough. With a mesoscopic signal level $S \sim 7$ photons, one has $P_b \sim 10^{-12}$, $P_b^{\rm het} \sim 10^{-3}$, and $P_b^{\rm ph} \sim 10^{-6}$. If the data arrives at a rate of 1 Gbps, Bob is likely to have 10^9 error-free bits in 1 second, while Eve would have at least (recall that she actually does not have the key even after her measurements) $\sim 10^6$ or $\sim 10^3$ errors in her 10^9 bits with heterodyne or the optimum-phase measurement (which has no known experimental realization). With the usual privacy amplification [23], the users can then generate $\sim 10^6$ or $\sim 10^3$ bits in a 1 second interval by eliminating Eve's information.

While these parameter values are not particularly remarkable due to the loose bound and have not been experimentally demonstrated, they illustrate the new KCQ principle of quantum key generation introduced in [3] that creates advantage via the difference between optimal quantum receiver performance with versus without knowledge of a secret key, which is more powerful than the previous BB84 principle since it does not rely on intrusion-level estimation to create advantage. Also note that due to the 3 dB advantage limitation of binary signaling (compare Eq. (18)and Eq.(16)), one may use the CPPM scheme [3] and its extensions instead of $\alpha\eta$-KG for key generation over long distances. Within the confines of binary signaling, the throughput, though not the advantage, can be greatly increased even for large S by moving the state close to the decision boundary. Detailed treatments will be given in the future.

The heterodyne attack on $\alpha\eta$ discussed above can of course be launched also on an $\alpha\eta$ Key Generation system. For parameter values, i.e., values of S, M and n, such that Eq. (15) holds, key generation with information-theoretic security is impossible in principle, since the Shannon limit (4) holds. This point is *missed* in all the criticisms of $\alpha\eta$ Key Generation [1, 18, 20], but was explicitly stated in the first version of Ref. [3]. It is at least implicit in Ref. [2] where we said the experiment has to be modified for key generation, and also mentioned the KCQ Key Generation Principle of optimal quantum receiver performance difference. One simple way to break the Shannon limit (4) and protect the key at the same time, is to employ DSR. As noted in Section 3.1, its use in $\alpha\eta$ direct encryption is expected to provide information-theoretic security for the key and at a level far exceeding the limit (4) for the data. We mention these possible approaches to make it clear that we were aware of the limitations of $\alpha\eta$ and that we need additional techniques to obtain unconditinal security.

4 The Lo-Ko Attacks

4.1 Review of Attacks in [1]

Ref. [1] first describes a known-plaintext attack on the original $\alpha\eta$ of [2] that can be launched when the channel loss allows Eve to have $2^{|K|}$ copies of the states Bob would receive. With $2^{|K|}$ copies, it is claimed that Eve can use each possible seed key to implement a decryption system similar to Bob's, and by comparing the outputs to the known-plaintext of some *unspecified* length s, can determine the key. Eve thus needs only beamsplitters and detectors similar to Bob's to undermine the system. We shall call this attack *Attack I* in the sequel. A variant of this attack is also described, in which Eve is assumed to know r $s-$bit sequences of plaintext, where $r(1-\eta) \geq 2^{|K|}\eta$. In other words, the channel transmittance η is such that Eve has in her possession, including repeated copies, $2^{|K|}$ ciphertext-states, each corresponding to a known $s-$bit sequence. What s needs to be is again unspecified. It is claimed that an exhaustive trial of keys would again pin down the key in this case. These attacks are also claimed to work, without *any* supporting argument, when the plaintext is not exactly known, but is drawn from a language, e.g., English.

It is further argued that even in just 3 dB loss (which is not required under our approach of granting Eve a copy of the quantum signal), a Grover quantum search (that will be called *Attack II*) would succeed in finding K under a known-plaintext attack when $n = \infty$, because then there is only a single possible key value that would give rise to the overall ciphertext-state from the known data X_n. This latter claim is in turn justified by the "asymptotic orthogonality" of the ciphertext-states corresponding to different key values, although exactly how

this asymptotic orthogonality occurs for different choices of the ENC box in Fig.1, including the LFSR used, is not described. The purpose of this argument is presumably to claim that a limiting statement such as (10) must be true, thus undermining the system under a known-plaintext attack *for large enough* n. When the plaintext X_n is not exactly known but is not completely random, i.e., under a statistical attack, such a result is also claimed to hold *without* any argument. Also, no estimate of the convergence rate in n is provided for either asymptotic orthogonality or for Eq.(10).

Ref. [1] then assumes that $\alpha\eta$ Key Generation, in which X_n is taken to be completely random as in all key-generation protocols (so that there is no possibility of a known-plaintext or statistical attack of any kind, at least before the generated key is used in another cipher), proceeds by utilizing the output bits $Y_n = X_n$ directly as key bits to XOR or "one-time pad" on new data. With known-plaintext attack on these new data, the X_n would be known and the previously described known-plaintext attacks I and II can be applied on the ciphertext-states to find K.

4.2 Response to Attacks

We will first respond to these attacks for direct encryption. The first gap in Attack I is that the length of known-plaintext n_1 needed to uniquely fix the key is not specified. From Subsection 2.3, we see that Eve needs length equal to the nondegeneracy distance n_d (11) of the ENC box of Fig.1 to fix the key from exact input-output pairs of the ENC box alone. Actually, $s = n_1$ needs to be larger than this nondegeneracy distance n_d due to the quantum noise randomization. Note also that the ENC box could be chosen to be degenerate, so that it does not even have a nondegeneracy distance and the key could never be pinned down. However, since the LFSR used in [2] is actually nondegenerate, we will not dwell on this point. As it stands, the attack is seriously incomplete without specifying what $s = n_1$ is or at least providing estimates of it. This corresponds to defect One in our Introduction.

Furthermore, Attack I requires the product $r(1-\eta)$ to be bigger than $\eta 2^{|K|}$, which implies either r or $1/\eta$ is at least exponential in $|K|/2$. Thus, Attack I can be thwarted by increasing the key length linearly, which is relatively easy. As an example, for the key length $|K| \sim 2\times 10^3$ used in [2], one needs a loss of 6×10^3 dB for $r = 1$, which corresponds to propagation over $\sim 3 \times 10^4$ km in the best available fiber, which has a loss of 0.2 dB/km. No conceivable one-stage communication line can be expected to operate over such a long distance. Any future improvements in the loss figure of fibers can only make Eve's task harder because the number of copies she can tap decreases along with the loss.

If the exponential loss requirement is replaced by that of an exponential length of data, it is equally fanciful. For the key length $|K| \sim 2\times 10^3$, $r = 2^{|K|}$ corresponds to $\sim 10^{600}$ bits of data. How could Eve input $\sim 10^{600}$ bits of data in a chosen-plaintext attack, or know $\sim 10^{600}$ bits in a known-plaintext attack? In any case, even if such large loss obtains, the attacker still has the problem of requiring an *exponential number* of devices (beamsplitters *and* detectors in this case) and doing an exponential amount of processing. Apart from size and time limitations mentioned in Section 2, it seems not possible to ever get $\sim 10^{600}$ devices corresponding to the above key length, considering that the total number of elementary particles in the universe is less than 10^{100}. This corresponds to defect Two in the Introduction. We should also mention that $\alpha\eta$ was claimed in [2] to be proved secure against known-plaintext attacks only in the

brute-force search sense and not information-theoretically, and so the above attacks do not contradict any claim in [2] even if they were successful.

Before proceeding to Attack II, we first distinguish the following *four* distinct kinds of statements that can be made on a quantity $\epsilon(n)$, basing roughly on the value of n being considered:

(i) The value of $\epsilon(n)$ at a finite n. This is of interest for a realistic implementation — typically $n \sim 10^2 - 10^4$ is the limit for joint processing of a single block.

(ii) The case expressed by a limit statement on some quantity of interest $\epsilon(n) \to 0$ *with* quantitative convergence rate estimate $0 \leq \epsilon(n) \leq f(n)$ for $n \geq N$ and some large enough N and a known function $f(n) \to 0$.

(iii) The case of the limit statement $\lim_{n\to\infty} \epsilon(n) = 0$ *without* convergence rate estimate. Thus, it is not known how large n needs to be for $\epsilon(n)$ to be below a certain given level ϵ_0.

(iv) The case of the value $\epsilon(\infty)$ *at* ∞. Note that the limiting value of $\epsilon(n)$ in Case (iii) above may be different from $\epsilon(\infty)$ due to failure of continuity at $n = \infty$.

Observe that the statements in Cases (i)-(iii) are, in that order, progressively weaker statements on the quantity of interest. Case (iv), however, is *independent* of the previous cases, and can be asserted by evaluating $\epsilon(\infty)$ by a route that does not even require $\epsilon(n)$ at finite n. In turn, knowing $\epsilon(\infty)$ does not allow one to make even a limit statement of the form of Case (iii) unless one can prove continuity at $n = \infty$. We have classified the above cases in order to delineate exactly what Lo and Ko can claim for their Attack II.

Let us now consider Attack II. The first obvious problem with the argument is that Eve does not need to attack the system if she already knows the entire $n \to \infty$ plaintext that will be transmitted using the particular seed key. Lo and Ko give *no* analysis of their attack for the relevant case in which the plaintext is partially known, i.e., for the case of a statistical attack (this includes the case of Eve knowing a fraction of the plaintext exactly) even in the $n \to \infty$ situation. A little thought will show that the oracle required in Grover search would have an implementation complexity that increases indefinitely with n, making it prohibitive to build in the $n \to \infty$ limit. In other words, the search complexity is not simply $\sim 2^{|K|/2}$ but rather increases with n as well. When there is more than one plaintext possible, Lo and Ko presumably intend to apply Grover search for each plaintext in turn. The number of such repeated applications would obviously grow indefinitely with n if Eve knows only a fraction of plaintext. In case they intend that a single Grover search be applied to cover all possible plaintexts, they need to produce a specific oracle that would work for this case and analyze its performance. The issue is more critical in actual practice, because it typically does not happen that Eve knows a large length of plaintext, let alone one that is arbitrarily long in the unquantified sense of (iii) above, which is what their attack entails. Furthermore, even if its n dependence is ignored, the $\sim 2^{|K|/2}$ complexity of the Grover's search makes it practically impossible to launch for $|K| \sim 2 \times 10^3$. Similar to Attack I, Attack II retains all the limitations of being exponential in the key length. This point is an instance of the second defect mentioned in Section 1.

Our second point regarding Attack II relates to the first general defect described in Section 1, namely lack of rigor. We claim that the "asymptotic orthogonality" in [1] is vague in that it is not specified which sense among (ii) - (iv) is meant. Moreover, even assuming that a Case (ii) statement holds, it cannot by itself be translated into even a limit statement of the form of Eq. (10). To see this, let us assume that the pairwise inner product between any of the $2^{|K|}$ ciphertext states $\{|\psi_k\rangle\}$ corresponding to a known plaintext encrypted with the different keys is upper bounded by a function $\epsilon(n)$. Let us take

$$\lim_{n\to\infty} \epsilon(n) = 0 \tag{19}$$

to mean "asymptotic orthogonality" in the sense of case (iii) or even (ii) above. For each n, we can in principle calculate the optimal probability of error $P_E(n)$ in discriminating the $2^{|K|}$ states, which, rather than the inner product, is the relevant quantity of *operational significance*. It is clear that $P_E(\infty) = 0$ in the sense (iv) above since $\epsilon(\infty) = 0$. However, to make the limit statement Eq. (10), one needs to further show from (19), the equivalent statement to (10) that

$$\lim_{n\to\infty} P_E(n) = 0, \tag{20}$$

perhaps from the claim that the probability of error is a *continuous* function of $\epsilon(n)$. Since the underlying Hilbert space is expanding with n and becoming nonseparable at $n = \infty$, it is not obvious whether continuity would hold, especially at $n = \infty$. In order to convince the reader that the above considerations indeed have real implications, we will in Section 5 use an asymptotic orthogonality argument to 'prove' coherent-state BB84 insecure for any non-zero loss.

Note that [1] does not actually prove "asymptotic orthogonality" in any of the senses (ii)-(iv). As discussed above in connection with Attack I, there are conditions required on the ENC box of Fig.1 for it to be true just in the sense (iv). On the other hand, we believe that (19) can be proved along with (20) under proper conditions on the ENC box. But one needs precise arguments to make clear the conditions of validity, which [1] does not provide.

Thirdly, even if their claim is correct as a *limit statement* of the form of Eq. (10), that result has no implication in practice. Indeed, an $\alpha\eta$ system with a LFSR for the ENC box in Fig.1 has a periodic running key output K' of period $n_p = 2^{|K|}/\log_2 M$. It is never meant to be used beyond such n_p, similar to the case of standard ciphers, even in the limit of no channel loss. A limiting claim such as Eq. (10), which falls under Case (iii) above, does not say anything about the insecurity of the actual system. These last two points are instances of the first and second defects described in Section 1, namely lack of rigor and insufficient attention to quantitative detail.

Finally, we stress that we were concerned in [2] only with exponential-complexity based security in direct encryption systems, which is as good as unconditional security for real systems. Also, we may mention that various added randomization techniques are introduced in [3] which would modify $\alpha\eta$ to become a random cipher even in the sense of quantum state. The security of such ciphers against known-plaintext attacks is an entirely open area of research.

We now respond to the Lo-Ko attacks on $\alpha\eta$ used as a key-generation system. First of all, we only mentioned in [2] the possibility in principle of using the system to do key generation

without giving a complete protocol. We did not imply that the system for the parameters in [2] and without any modifications would function for that purpose. Indeed, in light of the discussion in Sections 2 and 3, the Shannon limit (4) already applies to the original $\alpha\eta$ of [2] for all practical n. Thus, there is at most $|K|$-bits uncertainty in X_n to Eve, however long n is, leaving no possibility of key generation. Thus, Lo and Ko overlook the fact that fresh key *cannot* be generated *in principle* in their use of $\alpha\eta$ for key generation. Furthermore, even if the advantage creation condition is ignored, [1] does not include the usual step of privacy amplification that the users can apply to the output to make it a shorter uniformly-random key. This omission alone already *invalidates* their argument. These two points correspond to the defect Three of Section 1.

Since the attacks on $\alpha\eta$-KG are reduced in [1] to attacks on $\alpha\eta$ direct encryption, they also suffer the same problems as the attacks on direct encryption above. Indeed, one may conclude *a priori* that the attacks in [1], even if successful, do not contradict the claims in [2], and are indeed "outside the original design" because they are inapplicable in any realistic situation.

5 Attack on coherent-state BB84

It is claimed in [1] that "our attacks do not apply to BB84 or other standard QKD schemes where the quantum signals are strictly microscopic in the sense that there is (on average) at most one copy of the signal available." We will show that this is *false* by using an asymptotic orthogonality argument exactly parallel to that in [1] which will 'prove' that coherent-state BB84 using a classical error-correction code is insecure for *any* nonzero value of loss. Although we do not believe this latter statement to be true without qualification, we present this argument as an example to underscore the importance of rigorous reasoning before making the claim that $\alpha\eta$ Key Generation is insecure under Attack II in [1].

We denote by b the n-bit string that Alice intends to transmit to Bob in order to share a key. We denote by $|\psi_b\rangle$ the following product coherent state used to transmit b:

$$|\psi_b\rangle = \bigotimes_{i=1}^{i=n} |\alpha_{b_i}^{\beta_i}\rangle. \tag{21}$$

Here the superscript β_i defines which of the two BB84 bases is used for the ith transmission and the subscript b_i is the ith bit of b. The exact form of the states $|\alpha_{b_i}^{\beta_i}\rangle$ depends on the implementation. All that is relevant for our attack is to note the obvious fact that, for each β, the states $|\alpha_0^{\beta}\rangle$ and $|\alpha_1^{\beta}\rangle$ are distinct, and so $|\langle\alpha_0^{\beta}|\alpha_1^{\beta}\rangle| < 1$. The attack works as follows: When the channel transmittance is η, Eve simply splits a fraction $1-\eta$ of the energy using a beamsplitter and thus has in her possession the state

$$|\psi_b^E\rangle = \bigotimes_{i=1}^{i=n} |\sqrt{1-\eta}\alpha_{b_i}^{\beta_i}\rangle. \tag{22}$$

Eve holds this state in her quantum memory, while transmitting the remaining energy to Bob through a lossless line. Bob is thus totally oblivious of Eve's presence. She then listens to the public announcements of Alice and Bob, and discards along with Alice and Bob the bit positions where Bob observes a count in both or no detectors. She also rotates all the component states to the same basis according to the announcement of bases by Alice. Accordingly,

we may suppress the superscript β_i. Next, according to the protocol, Alice and Bob estimate the error rate on a subset of their choice. Let us now assume that n refers to the remaining subset. If the fraction of errors in the test set is under the error threshold δ, Alice and Bob select an (n, k, d) code with $d > 2\delta n$ to correct the errors on the remaining bits. After the announcement of the syndrome of b with respect to the chosen code, the number of possible b's goes to $M = 2^k$ rather than the original number of possibilities 2^n. Eve listening on the public channel can determine which possibilities remain, and can launch a powerful attack, as seen in the following.

The inner product of Eve's states corresponding to two admissible bit sequences b and b' is

$$|\langle\psi_b^E|\psi_{b'}^E\rangle| = \prod_{i=1}^{n} |\langle\sqrt{1-\eta}\alpha_{b_i}|\sqrt{1-\eta}\alpha_{b_i'}\rangle| = \epsilon^{\delta_H(b,b')} \leq \epsilon^d < \epsilon^{2\delta n}. \tag{23}$$

Here $\delta_H(b, b')$ is the Hamming distance between the strings b and b', which is restricted to be at least the distance of the code d and

$$\epsilon = |\langle\sqrt{1-\eta}\alpha_0|\sqrt{1-\eta}\alpha_1\rangle| < 1. \tag{24}$$

Since ϵ is strictly less than 1, Eq. (23) shows that the M possibilities become orthogonal in the senses (ii)-(iv) of the previous section. One thus has the result that the *probability of error* on b, $P_E(\infty) = 0$ since Eve can distinguish orthogonal states without error. If one pulls this case (iv) statement to a case (iii) limiting statement of Eve's error probability $P_E(n)$ on b, parallel to the argument in [1] which takes (19) to (20), it would imply that the system would become insecure for large n and any nonzero value of loss!

We stress that the above result cannot be correct for all values of the signal energy, channel loss and other parameters such as the code rate k/n, no matter how large n is. One reason for doubting its universal correctness is that it would contradict the known classical information transmission capacity of a lossy bosonic channel [24]. However, the *line of argument* is exactly in parallel to that of [1]. We give it here to demonstrate the consequences of jumping to a limiting statement from an $n = \infty$ statement on the error probability. However, we do believe that the above attack has not been accounted for in the security proofs in the literature. Indeed, we agree with [1] that it is "interesting to study the subtle loopholes in existing schemes," and that one should "never under-estimate the effort and ingenuity that your adversaries are willing to spend on breaking your codes."

6 Other comments on Lo-Ko [1]

In this section we comment on some other claims in [1].

(i) The authors of [1] seem to believe that optical amplifiers can be and are used to compensate for an arbitrary amount of loss provided mesoscopic signal levels are used. The supposed existence of such high-loss links in optical systems is perhaps the reason that they state that their "(beamsplitter) attack can to some extent, be implemented with current technology." and that "our attacks severely limit the extent of such optical amplification." In reality, however, optical amplifiers are noisy (i.e., degrade the probability of error for all measurements except heterodyne [25]) irrespective of signal strength. Thus, in practice, in order to retain an acceptable signal-to-noise ratio at the output,

optical amplifiers are placed at periodic intervals in a long-distance fiber link, with the first optical amplifier being inserted much before the channel transmittance decays to $\sim 2^{-|K|}$ for $|K|$ in the range of $|K| \sim 1000$. So, Lo and Ko need to specify exactly how they would proceed to attack such an optically-amplified line for which each section has $\eta >> 2^{-|K|}$.

Optical-amplifier noise actually provides limits of operation for both $\alpha\eta$ and $\alpha\eta$-KG. For $\alpha\eta$-KG, the optical amplifier noise would limit the attainable advantage needed for key generation. For $\alpha\eta$ direct encryption, amplifier noise is a limit when there is too much of it, but it is a help against Eve when present in a moderate amount. See for example [17]. The full story of loss and amplifiers in $\alpha\eta$ systems depends on implementation and additional security techniques to be deployed on top of basic $\alpha\eta$, and is yet to be told.

(ii) We do not believe that their attacks can be implemented to *any* useful extent with current *or* future technology, as they require exponential resources and processing.

(iii) It was pointed out in [1] that "mesoscopic states for quantum key distribution was first proposed by Bennett and Wiesner [26] in 1996." The principle underlying that scheme is the usual BB84 type disturbance/information tradeoff, which is radically different from our KCQ principle. Indeed, the mesoscopic nature of the signal in that scheme is a hindrance and not a help on the operation of the cryptosystem due to sensitivity problems. This is because it is not the absolute strength of the signals that matters, but rather whether they are *distinguishable*. The large signals in [26] still have only one photon average difference between them. As the large signal gets attenuated in a lossy line, the one-photon difference also gets attenuated correspondingly. Thus, as compared to the small signal case, these large signals are distinguishable at the receiver with the same absolute difficulty, but with a bigger relative difficulty since the signal level difference is now a much smaller percentage of the absolute level.

7 Conclusions

There are two main claims in [1] against the original $\alpha\eta$ cryptosystem of [2, 3].

(1) It is broken in high loss channels by a beamsplitter attack (Attack I) and in 3 dB loss by a quantum search (Attack II) when the attacker knows a sufficiently long plaintext for Attack I and infinitely long plaintext for Attack II. The lack of security is taken in the information-theoretic sense that the seed key K could be uniquely determined.

(2) If the output of an $\alpha\eta$ Key Generation ($\alpha\eta$-KG) system is directly used as the key in a "one-time pad" cipher, then a known-plaintext attack on that cipher would allow one to launch the above known-plaintext attacks on $\alpha\eta$-KG.

Our detailed response has been given in this paper, which describes the proper framework for discussing these attacks and shows that the arguments in [1] fail at many levels. A brief summary of our response follows:

For direct encryption, Attack I requires either loss that is exponentially large in the key length or knowledge of an exponentially long sequence of plaintext, which are both unrealistic. Attack II, by *requiring* n to be infinite, is not applicable as the original $\alpha\eta$ is designed to run

for a finite n. That attack also contains gaps in the reasoning for making even a limiting insecurity statement. While it is claimed that these attacks work when just the statistics of the plaintext is known, it is not described how it would even proceed, not to mention its quantitative performance. Also, the attacks, even if successful, do not undermine our claims in [2] of exponential assisted brute-force search complexity under known-plaintext attacks.

The attacks on $\alpha\eta$ as a key-generation system are founded on a key-generation protocol created by Lo and Ko, since no key-generation system was detailed in [2]. Their key-generation protocol omits the crucial step of privacy amplification before the generated key is used in an encryption system. In addition, the attacks are not relevant for the security of $\alpha\eta$ with the parameters of [2] since, for information-theoretic security of the key studied in [1], the heterodyne attack described in [3] and this paper and not recognized in [1] prevents the original $\alpha\eta$ from generating fresh keys due to the Shannon limit.

Perhaps more significantly, we have described various security features of $\alpha\eta$ that appear to be widely misunderstood, partly because little is known on the corresponding classical or standard cryptosystems. We hope this paper explains our new approach sufficiently to dispel misunderstandings, and at the same time highlights many important considerations on quantum cryptography in action.

Acknowledgments

We would like to thank T. Banwell, H. Brandt, G.M. D'Ariano, M. Foster, M. Goodman, O. Hirota, D. Hughes, C. Liang, D. Nicholson, M. Ozawa, J. Smith, P. Toliver, and K. Yamazaki for many useful discussions during the continuing development of $\alpha\eta$.

This work was supported under DARPA grant F30602-01-2-0528.

References

1. Lo and Ko, "Some attacks on quantum-based cryptographic protocols", Quant. Inform. and Comp. *6* (2005) 040-047.
2. G. Barbosa, E. Corndorf, P. Kumar, H.P. Yuen, "Secure communication using mesoscopic coherent states", Phys. Rev. Lett. 90 (2003) 227901.
3. H.P. Yuen, "KCQ: A new approach to quantum cryptography I. General principles and qumode key generation", quant-ph/0311061.
4. R. Nair, H.P. Yuen, E. Corndorf, T. Eguchi, P. Kumar, "Quantum Noise Randomized Ciphers", quant-ph/0603263; Submitted to PRA.
5. H.P. Yuen, P. Kumar, E. Corndorf, R. Nair, "Comment on 'How much security does Y-00 protocol provide us?"', Phys. Lett. A, 346 (2005) 1-6; quant-ph/0407067.
6. O. Hirota, M. Sohma, M. Fuse, and K. Kato, 'Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme", Phys. Rev. A. 72 (2005) 022335; quant-ph/0507043.
7. D.R. Stinson, *Cryptography: Theory and Practice*, Chapman and Hall/CRC, 2nd ed, 2002.
8. J.L. Massey, "An introduction to contemporary cryptology", Proc. IEEE, 76 (1988) 533-549.
9. C. Shannon, "Communication theory of secrecy systems", Bell Syst. Tech. J. 28 (1949) 656–715.
10. U. Maurer, IEEE Trans. IT, vol. 39, No. 3, 1993, "Secret Key Agreement by Public Discussion from Common Information", pp. 733-742.
11. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum Cryptography", Rev. Mod. Phys. 74, 145 (2002).

12. H.P. Yuen, "Direct Use of Secret Key in Quantum Cryptography", quant-ph/0603264; Submitted to PRL.
13. H.N. Jendahl, Y.J.B. Kuhn, J.L. Massey, "An information- theoretic treatment of homophonic substitution", Advances in Cryptology -EUROCRYPT '89, Lect. Notes in Comp. Science 434, 382-394, 1990, Springer-Verlag, Berlin.
14. Ch.G. Gunther, "A universal algorithm for homophonic coding", Advances in Cryptology - EUROCRYPT '88, Lect. Notes in Comp. Sci 330, 405-414, 1988, Springer-Verlag.
15. E. Corndorf, G. Barbosa, C. Liang, H. Yuen, P. Kumar, "High-speed data encryption over 25km of fiber by two-mode coherent-state quantum cryptography", Opt. Lett. 28, 2040-2042, 2003.
16. E. Corndorf, C. Liang, G.S. Kanter, P. Kumar, and H.P. Yuen, "Quantum-noise–protected data encryption for WDM fiber-optic networks", Phys. Rev. A 71 (2005) p. 062326.
17. C. Liang, G.S. Kanter, E. Corndorf, and P. Kumar, "Quantum noise protected data encryption in a WDM network", Photonics Tech. Lett. 17, pp. 1573-1575, 2005.
18. T. Nishioka, T. Hasegawa, H. Ishizuka, K. Imafuku, H. Imai, "How much security does Y-00 protocol provide us?", Phys. Lett. A 327 (2004) 28-32; quant-ph/0310168.
19. T. Nishioka, T. Hasegawa, H. Ishizuka, K. Imafuku, H. Imai, "Reply to: 'Comment on: How much security does Y-00 protocol provide us?' ", Phys. Lett. A 346 (2005), 7-16.
20. Z. Yuan and A. Shields, "Comment on 'Secure Communication using mesoscopic coherent states', Barbosa et al, Phys. Rev. Lett. 90, 227901", Phys. Rev. Lett. 94, 048901(2005). See also our response [21].
21. H.P. Yuen, E. Corndorf, G. Barbosa, P. Kumar, Phys. Rev. Lett. 94, 048902 (2005).
22. C. Helstrom, *Quantum Detection and Estimation Theory*, Academic, New York, 1976.
23. C. Bennett, G. Brassard, C. Crépeau, U. Maurer, "Generalized privacy amplification", IEEE Trans. IT 41 (1995) 1915–1922.
24. V. Giovanetti, S. Guha, S. Lloyd, L. Maccone, J.H. Shapiro, H.P. Yuen, "Classical capacity of the lossy bosonic channel: the exact solution", Phys. Rev. Lett. 92, 027902 (2004).
25. H.P. Yuen, "Design of transparent optical networks using novel quantum amplifiers and sources", Opt. Lett. vol.12, p.789, 1987.
26. C.H. Bennett, and S.J. Wiesner, "Quantum key distribution using non-orthogonal macroscopic states", US Patent Number 5,515,438 (1996), Available online at www.uspto.gov.

Appendix A – Security Against Known-Plaintext Attack

In this appendix, we provide a brief quantitative discussion of known-plaintext attacks on random and nonrandom ciphers that is not available in the literature. For nonrandom ciphers, we have the following

Propositon A

If a nonrandom cipher has nondegeneracy distance n_d, then it is broken by a known-plaintext attack with data length $n = n_d$. $n = n_d$ is also the smallest n for which the cipher is broken with probability 1.

Proof: For any three joint random vectors X_n, Y_n, K, we have the identity

$$H(Y_n|X_n) + H(K|X_nY_n) = H(K|X_n) + H(Y_n|KX_n). \tag{25}$$

For a nonrandom cipher, $H(Y_n|KX_n) = 0$. In general, $H(K|X_n) \leq H(K)$. Thus, $H(K|X_nY_n) = 0$ at any n satisfying Eq. (10) or Eq. (11) and vice versa. From its definition, n_d is thus the smallest data length at which the key is found for any given x_n.

A similar result clearly holds for chosen plaintext attacks. Note that if we consider the equation

$$H(X_n|Y_n) + H(K|X_nY_n) = H(K|Y_n) + H(X_n|KY_n), \tag{26}$$

then under (3), a random cipher is broken by a known-plaintext attack if $H(X_n|Y_n)$ satisfies the Shannon limit (4) with equality. However, if one is satisfied with using entropies as quantitative measures of security, one may have a situation where

$$\inf_n H(X_n|Y_n) = \lambda_1 H(K), \tag{27}$$

$$\inf_n H(K|X_nY_n) = \lambda_2 H(K), \tag{28}$$

$$\inf_n H(K|Y_n) = (\lambda_1 + \lambda_2) H(K), \tag{29}$$

under the constraint (26) where $0 < \lambda_1, \lambda_2 < 1$ and $\lambda_1 + \lambda_2 \leq 1$. (27-29) may still provide satisfactory levels of security if $|K|$ is long enough, and if Eve's information on the data bounded by $\lambda_1 H(K)$ does not help Eve to reduce her uncertainty on the rest of the data below whatever designed level (We cannot enter into a detailed discussion, as one problem of using entropies as quantitative measures of security shows up here). While we have not given any specific random cipher with such characteristics proven, it has not been ruled out either. On the other hand, if redundant key use or degeneracy is avoided for nonrandom ciphers, then Proposition A applies. A detailed development will be given elsewhere.